3. Mathematical Induction

3.1. First Principle of Mathematical Induction. Let $P(n)$ be a predicate with domain of discourse (over) the natural numbers $\mathbb{N} = \{0, 1, 2, ...\}$. If

(1) $P(0)$, and
(2) $P(n) \to P(n+1)$

then $\forall n P(n)$.

Terminology: The hypothesis $P(0)$ is called the **basis step** and the hypothesis, $P(n) \to P(n+1)$, is called the **induction (or inductive) step**.

Discussion

The Principle of Mathematical Induction is an axiom of the system of natural numbers that may be used to prove a quantified statement of the form $\forall n P(n)$, where the universe of discourse is the set of natural numbers. The principle of induction has a number of equivalent forms and is based on the last of the four Peano Axioms we alluded to in *Module 3.1 Introduction to Proofs*. The axiom of induction states that if S is a set of natural numbers such that (i) $0 \in S$ and (ii) if $n \in S$, then $n + 1 \in S$, then $S = \mathbb{N}$. This is a fairly complicated statement: Not only is it an "if ..., then ..." statement, but its hypotheses *also* contains an "if ..., then ..." statement (if $n \in S$, then $n + 1 \in S$). When we apply the axiom to the truth set of a predicate $P(n)$, we arrive at the *first principle of mathematical induction* stated above. More generally, we may apply the principle of induction whenever the universe of discourse is a set of integers of the form $\{k, k + 1, k + 2, \dots\}$ where k is some fixed integer. In this case it would be stated as follows:

Let $P(n)$ be a predicate over $\{k, k + 1, k + 2, k + 3, \dots\}$, where $k \in \mathbb{Z}$. If

(1) $P(k)$, and
(2) $P(n) \to P(n+1)$

then $\forall n P(n)$.

In this context the "for all n", of course, means for all $n \geq k$.

REMARK 3.1.1. *While the principle of induction is a very useful technique for proving propositions about the natural numbers, it isn't always necessary. There were a number of examples of such statements in Module 3.2 Methods of Proof that were proved without the use of mathematical induction.*

Why does the principle of induction work? This is essentially the domino effect. Assume you have shown the premises. In other words you know $P(0)$ is true and you know that $P(n)$ implies $P(n+1)$ for any integer $n \geq 0$.

Since you know $P(0)$ from the basis step and $P(0) \to P(1)$ from the inductive step, we have $P(1)$ (by *modus ponens*).

Since you now know $P(1)$ and $P(1) \to P(2)$ from the inductive step, you have $P(2)$.

Since you now know $P(2)$ and $P(2) \to P(3)$ from the inductive step, you have $P(3)$.

And so on ad infinitum (or ad nauseum).

3.2. Using Mathematical Induction.

Steps

1. Prove the basis step.
2. Prove the inductive step
   (a) Assume $P(n)$ for arbitrary n in the universe. This is called the **induction hypothesis**.
   (b) Prove $P(n+1)$ follows from the previous steps.

Discussion

Proving a theorem using induction requires two steps. First prove the basis step. This is often easy, if not trivial. Very often the basis step is $P(0)$, but sometimes, when the universal set has k as its least element, the basis step is $P(k)$. Be careful to start at the correct place.

Next prove the inductive step. *Assume* the induction hypothesis $P(n)$ is true. You do *not try to prove the induction hypothesis.* Now you prove that $P(n+1)$ *follows* from $P(n)$. In other words, you will use the truth of $P(n)$ to show that $P(n+1)$ must also be true.

Indeed, it may be possible to prove the implication $P(n) \to P(n+1)$ even though the predicate $P(n)$ is actually false for every natural number n. For example, suppose

$P(n)$ is the statement $n = n - 1$, which is certainly false for all n. Nevertheless, it is possible to show that *if* you assume $P(n)$, then you can correctly deduce $P(n+1)$ by the following simple argument:

PROOF. If $n = n - 1$, then, after adding 1 to both sides, $n + 1 = (n - 1) + 1 = (n + 1) - 1$. Thus $P(n) \to P(n + 1)$. □

It is easy at this point to think you are assuming what you have to prove (circular reasoning). You must keep in mind, however, that when you are proving the implication $P(n) \to P(n + 1)$ in the induction step, you are not proving $P(n)$ directly, as the example above makes clear, so this is not a case of circular reasoning. To prove an implication, all you need to show is that *if the premise is true* then the conclusion is true. Whether the premise is actually true at this point of an induction argument is completely irrelevant.

EXERCISE 3.2.1. *Notice in the above example that, while we proved* $\forall n[P(n) \to P(n + 1)]$, *we did not prove* $\forall n P(n)$. *Why?*

3.3. Example 3.3.1.

EXAMPLE 3.3.1. *Prove:* $\displaystyle\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$ *for* $n = 0, 1, 2, 3, \ldots$

PROOF. Let $P(n)$ be the statement $\displaystyle\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$.

1. Basis Step, $n = 0$:

   Prove $\displaystyle\sum_{i=0}^{0} i = 0(0 + 1)/2$.

   Proof: $\displaystyle\sum_{i=0}^{0} i = 0$ and $0(0 + 1)/2 = 0$

   Thus, $P(0)$.
2. Induction Step: Let $n \in \mathbb{N}$. At this step we are fixing an arbitrary integer $n \geq 0$ and making the following assumption for this fixed n. We then show the statement $P(n+1)$ must also be true. In general, we assume the induction hypothesis for an integer at least as large as the integer used in the basis case.

   (i) Assume $P(n)$: $\displaystyle\sum_{i=0}^{n} i = n(n + 1)/2$, for some integer $n \geq 0$.

(ii) Use the induction hypothesis to prove

$$\sum_{i=0}^{n+1} i = (n+1)((n+1)+1)/2.$$

Proof: Write out the sum on the left hand side of the statement to be proven.

$$\begin{aligned}
\sum_{i=0}^{n+1} i &= 0+1+2+3+\cdots+n+(n+1) \\
&= (0+1+2+3+\cdots+n)+(n+1) \\
&= \underbrace{\left(\sum_{i=0}^{n} i\right)}_{} +(n+1) \\
&\qquad \text{equal by the induction hypothesis} \\
&= \overbrace{\left[\frac{n(n+1)}{2}\right]}^{} +(n+1) \\
&= \frac{n^2+n+2n+2}{2} = \frac{n^2+3n+2}{2} \\
&= \frac{(n+1)(n+2)}{2} \\
&= \frac{(n+1)((n+1)+1)}{2}
\end{aligned}$$

By the principle of mathematical induction it follows that $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$ for all natural numbers n.

□

Discussion

Example 3.3.1 is a classic example of a proof by mathematical induction. In this example the predicate $P(n)$ is the statement

$$\sum_{i=0}^{n} i = n(n+1)/2.$$

[Recall the "Sigma-notation": $\sum_{i=k}^{n} a_i = a_k + a_{k+1} + \cdots + a_n$.]

It may be helpful to state a few cases of the predicate so you get a feeling for whether you believe it's true and for the differences that occur when you change n. But keep in mind that exhibiting a few cases *does not constitute a proof.* Here are a few cases for Example 3.3.1. Notice what happens to the summation (left-hand side) as you increase n.

$P(0)$: $\sum_{i=0}^{0} i = 0 = 0(0+1)/2$.

$P(1)$: $\sum_{i=0}^{1} i = 0 + 1 = 1(1+1)/2$.

$P(2)$: $\sum_{i=0}^{2} i = 0 + 1 + 2 = 2(2+1)/2$.

$P(3)$: $\sum_{i=0}^{3} i = 0 + 1 + 2 + 3 = 3(3+1)/2$.

In the basis step of an induction proof, you only need to prove the first statement above, but not the rest.

In the induction step you assume the induction hypothesis, $P(n)$, for some arbitrary integer $n \geq 0$. Write it out so you know what you have to work with. Then write out $P(n+1)$ so you can see what you need to prove. It will be easier to see how to proceed if you write both of these down. (A common mistake students make is to think of $P(n)$ as a particular expression (say, $P(n) = \sum_{i=0}^{n} i$) instead of as a *sentence*: $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$.) Once you have written down the induction hypothesis and what you need to prove, look for a way to express part of $P(n+1)$ using $P(n)$. In this example we use the summation notation $\sum_{i=0}^{n+1} a_i = (\sum_{i=0}^{n} a_i) + a_{n+1}$. This is a typical step when proving a summation formula of this type. After rewriting $\sum_{i=0}^{n+1} i$ this way, we can apply the induction hypothesis to substitute $n(n+1)/2$ for $\sum_{i=0}^{n} i$. Note that you should use the induction hypothesis at some point in the proof. Otherwise, it is not really an induction proof.

EXERCISE 3.3.1. *Prove:* $\sum_{i=1}^{n}(2i-1) = 1+3+5+\cdots+(2n-1) = n^2$, *for all* $n \geq 1$.

EXERCISE 3.3.2. *Prove:* $\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}$

EXERCISE 3.3.3. *Prove* $\sum_{k=1}^{n} 3 \cdot 2^{k-1} = 3(2^n - 1)$

3.4. Example 3.4.1.

EXAMPLE 3.4.1. *Prove:* $5n+5 \leq n^2$ *for all integers* $n \geq 6$.

PROOF. Let $P(n)$ be the statement $5n+5 \leq n^2$.

1. Basis Step, $n = 6$: Since $5(6)+5 = 35$ and $6^2 = 36$ this is clear. Thus, $P(6)$.
2. Induction Step: Assume $P(n)$: $5n+5 \leq n^2$, for some integer $n \geq 6$. Use the induction hypothesis to prove $5(n+1)+5 \leq (n+1)^2$.

   First rewrite $5(n+1)+5$ so that it uses $5n+5$:
   $$5(n+1)+5 = (5n+5)+5.$$
   By the induction hypothesis we know
   $$(5n+5)+5 \leq n^2+5.$$
   Now we need to show
   $$n^2+5 \leq (n+1)^2 = n^2+2n+1.$$
   To see this we note that when $n \geq 2$,
   $$2n+1 \geq 2 \cdot 2 + 1 = 5$$
   (and so this is also valid for $n \geq 6$).

   Thus, when $n \geq 6$,
   $$\begin{aligned} 5(n+1)+5 &= (5n+5)+5 \\ (5n+5)+5 &\leq n^2+5 \\ n^2+5 &\leq n^2+2n+1 \\ n^2+2n+1 &= (n+1)^2. \end{aligned}$$

Which shows $5(n+1)+5 \leq (n+1)^2$. By the principle of mathematical induction it follows that $5n+5 \leq n^2$ for all integers $n \geq 6$.

□

Discussion

In Example 3.4.1, the predicate, $P(n)$, is $5n+5 \leq n^2$, and the universe of discourse is the set of integers $n \geq 6$. Notice that the basis step is to prove $P(6)$. You might also observe that the statement $P(5)$ is false, so that we can't start the induction any sooner.

In this example we are proving an *inequality* instead of an equality. This actually allows you more "fudge room", but sometimes that extra freedom can make it a bit more difficult to see what to do next. In this example, the hardest part, conceptually, is recognize that we need *another* inequality, $5 \leq 2n+1$, which holds whenever $n \geq 2$. A good approach to showing $f(n+1) \leq g(n+1)$ is to start with $f(n+1)$, think of a way express $f(n+1)$ in terms of $f(n)$ so that you can use the induction hypothesis, then find ways to get to $g(n+1)$ using further equalities or inequalities (that go in the right direction!).

In the induction step we use the fact that if you know $a \leq b$, then $a+5 \leq b+5$. The induction hypothesis gives us an inequality. Then we add 5 to both sides of that inequality prove $P(n+1)$.

Remark 3.4.1. *In proving an identity or inequality, you don't always have to start with the left side and work toward the right. In Example 3.4.1 you might try to complete the induction step by starting with* $(n+1)^2$ *and showing that it is greater than or equal to* $5(n+1)+5$. *The steps would go as follows:*

$$\begin{aligned}
(n+1)^2 &= n^2+2n+1 \\
n^2+2n+1 &\geq (5n+5)+2n+1 && \textit{by the induction hypothesis} \\
(5n+5)+2n+1 &= 5(n+1)+2n+1 \\
5(n+1)+2n+1 &\geq 5(n+1)+5 && \textit{if } n \geq 2
\end{aligned}$$

With this approach the place where the induction hypothesis comes in as well as the fact that we need the inequality $2n+1 \geq 5$ *for* $n \geq 2$ *are, perhaps, a little more transparent.*

Exercise 3.4.1. *Prove:* $2n+1 \leq 2^n$, *for all* $n \geq 3$. *Establish the induction step in two ways, as suggested in the remark above. [Hint:* $2^n+2^n = 2 \cdot 2^n = 2^{n+1}$.*]*

EXERCISE 3.4.2. *Prove: $n^2 + 3 \le 2^n$, for all $n \ge 5$. [Hint: Look for a place to use the inequality in the exercise above in the induction step.]*

3.5. Example 3.5.1.

EXAMPLE 3.5.1. *Prove: A set with n elements, $n \ge 0$, has exactly 2^n subsets.*

PROOF. Let $P(n)$ be the statement "A set with n elements has 2^n subsets."

1. Basis Step, $n = 0$: The only set with 0 elements is the empty set, $\emptyset$, which has exactly one subset, namely, $\emptyset$. We also have $2^0 = 1$, therefore a set with 0 elements has exactly 2^0 subsets. Thus $P(0)$.
2. Induction Step: Let $n \in \mathbb{N}$. Assume $P(n)$: every set with n elements has 2^n subsets. Use the induction hypothesis to prove a set with $n+1$ elements has 2^{n+1} subsets.

   Suppose A is a set with $n+1$ elements, say, $A = \{a_1, a_2, \ldots, a_n, a_{n+1}\}$. Let B be the subset $\{a_1, a_2, \ldots, a_n\}$ of A. Since B has n elements, we can apply the induction hypothesis to B, which says that B has exactly 2^n subsets. Each subset S of B corresponds to exactly two subsets of A, namely, S and $S \cup \{a_{n+1}\}$. But every subset of A is of one of these two forms; hence, A has exactly twice as many subsets as B. Thus, A has exactly $2 \cdot 2^n = 2^{n+1}$ subsets.

By the principle of mathematical induction it follows that a set with n elements has exactly 2^n subsets for all $n \ge 0$. □

Discussion

EXERCISE 3.5.1. *Let $A = \{a, b, c, d, e\}$ and $B = \{a, b, c, d\}$. List all the subsets of A in one column and all the subsets of B in another column. Draw a line connecting every subset of A to a subset from B to demonstrate the 2 to 1 correspondence used in the previous proof. Note that an example such as this does not prove the previous Theorem, but it does help to illustrate the tools used.*

Induction is used in a variety of situations. In Example 3.5.1 induction is used to establish a formula for the number of subsets of a set with n elements. In this case we are not trying to prove an equality in the sense of establishing an identity, as with the summation examples. The induction step involves more "pure reasoning" than algebraic manipulation. We have to devise a strategy to count the number of subsets of a set with $n+1$ elements, given that we know a formula for the number of subsets of a set with n elements. Having devised a strategy, we then need to show that the formula works for a set with $n+1$ elements as well. Once you begin to be proficient in constructing inductive proofs of this type, you are well on your way to a complete understanding of the induction process.

EXERCISE 3.5.2. *Prove: For all $n \geq 0$, a set with n elements has $\dfrac{n(n-1)}{2}$ subsets with exactly two elements. [Hint: In order to complete the induction step try to devise a strategy similar to the one used in the example in Example 3.5.1. It is interesting to observe that the formula works for sets with fewer than 2 elements.]*

Here is another type of problem from number theory that is amenable to induction.

EXAMPLE 3.5.2. *Prove: For every natural number n, $n(n^2+5)$ is a multiple of 6 (i.e. $n(n^2+5)$ equals 6 times some integer).*

PROOF. Let $P(n)$ be the statement $n(n^2+5)$ is a multiple of 6.

1. Basis Step, $n = 0$: $0(0^2+5) = 0 = 0 \cdot 6$. Thus $P(0)$.
2. Induction Step: Suppose $n \in \mathbb{N}$, and suppose $n(n^2+5)$ is divisible by 6. Show that this implies $(n+1)((n+1)^2+5)$ is divisible by 6. In order to use the inductive hypothesis, we need to extract the expression $n(n^2+5)$ out of the expression $(n+1)((n+1)^2+5)$.
$$\begin{aligned}
(n+1)((n+1)^2+5) &= n((n+1)^2+5) + 1 \cdot ((n+1)^2+5) \\
&= n(n^2+2n+1+5) + (n^2+2n+1+5) \\
&= n(n^2+5) + n(2n+1) + (n^2+2n+6) \\
&= n(n^2+5) + 2n^2 + n + n^2 + 2n + 6 \\
&= n(n^2+5) + 3n^2 + 3n + 6 \\
&= n(n^2+5) + 3n(n+1) + 6
\end{aligned}$$

By the induction hypothesis, the first term on the right-hand side, $n(n^2+5)$, is a multiple of 6. Notice that n and $n+1$ are consecutive integers; hence, one of them is even. Thus, $n(n+1)$ is a multiple of 2, and so $3n(n+1)$ is a multiple of 6. If we write $n(n^2+5) = 6k$ and $3n(n+1) = 6\ell$, then
$$(n+1)((n+1)^2+5) = n(n^2+5) + 3n(n+1) + 6 = 6k + 6\ell + 6 = 6(k+\ell+1)$$

so $(n+1)((n+1)^2+5)$ is a multiple of 6. Thus, we have shown $P(n) \to P(n+1)$.

By the principle of mathematical induction, $n(n^2+5)$ is a multiple of 6 for every $n \geq 0$. □

You may have noticed that in order to make the inductive step work in most of the examples and exercises we have seen so far, the restriction placed on n is actually used, either implicitly or explicitly, whereas in the previous example it was not. (At no place in the inductive step above did we need the assumption that $n \geq 0$.) This leaves open the possibility that $n(n^2+5)$ is a multiple of 6 for (some/all?) integers $n < 0$ as well. Checking some cases, we see for

$n = -1$: $n(n^2+5) = (-1)((-1)^2+5) = -6$ is a multiple of 6,

$n = -2$: $n(n^2+5) = (-2)((-2)^2+5) = -18$ is a multiple of 6,

$n = -3$: $n(n^2+5) = (-3)((-3)^2+5) = -42$ is a multiple of 6,

$n = -4$: $n(n^2+5) = (-4)((-4)^2+5) = -84$ is a multiple of 6.

Exercise 3.5.3. *Use mathematical induction to prove that $n(n^2+5)$ is a multiple of 6 for all $n \leq 0$. [Hint: You will have to find the appropriate predicate $P(k)$.]*

Exercise 3.5.4. *Prove $5^{2n-1}+1$ is divisible by 6 for $n \in \mathbb{Z}^+$.*

Exercise 3.5.5. *Prove $a-b$ is a factor of $a^n - b^n$. Hint: $a^{k+1} - b^{k+1} = a(a^k - b^k) + b^k(a-b)$.*

Exercise 3.5.6. *The following is an incorrect "proof" that any group of n horses are the same color. What is the error in the proof?*

Proof. The basis case is certainly true since any group of 1 horse is the same color. Now, let $n \in \mathbb{Z}^+$ and assume any group of n horses are the same color. We need to show any group of $n+1$ horses is the same color. Let $\{h_1, h_2, \ldots, h_{n+1}\}$ be a set of $n+1$ horses. The set $\{h_1, h_2, \ldots, h_n\}$ is a set of n horses and so these horses are the same color. Moreover, the set $\{h_2, h_3, \ldots, h_{n+1}\}$ is a set of n horses, so they are all the same color. Therefore the set of horses $\{h_1, h_2, \ldots h_{n+1}\}$ must all be the same color.

□

3.6. The Second Principle of Mathematical Induction. Let k be an integer, and let $P(n)$ be a predicate whose universe of discourse is the set of integers $\{k, k+1, k+2, ...\}$. Suppose

1. $P(k)$, and
2. $P(j)$ for $k \leq j \leq n$ implies $P(n+1)$.

Then $\forall n P(n)$.

Discussion

The second principle of induction differs from the first only in the form of the induction hypothesis. Here we assume not just $P(n)$, but $P(j)$ for all the integers j between k and n (inclusive). We use this assumption to show $P(n+1)$. This method of induction is also called **strong mathematical induction**. It is used in computer science in a variety of settings such as proving recursive formulas and estimating the number of operations involved in so-called "divide-and-conquer" procedures.

EXERCISE 3.6.1. *Prove the first principle of mathematical induction is equivalent to the second principle of mathematical induction.*

EXAMPLE 3.6.1. *Prove: Every integer $n \geq 2$ can be expressed as a product of one or more prime numbers. A prime number is defined to be an integer greater than one that is only divisible by itself and one.*

PROOF. Recall that a prime number is an integer ≥ 2 that is only divisible by itself and 1. (The number 1 is not considered to be prime.)

Let $P(n)$ be the predicate "n can be expressed as a product of prime numbers."

1. Basis Step, $n = 2$: Since 2 is prime, 2 can be expressed as a product of prime numbers in a trivial way (just one factor). Thus, $P(2)$ is true.
2. Induction Step: Let n be an integer with $n \geq 2$. Suppose that every integer j, $2 \leq j \leq n$, can be expressed as a product of prime numbers.
   The integer $n+1$ is either a prime number or it is not.
   Case 1. If $n+1$ is a prime number, then it is a product of prime numbers in a trivial way.
   Case 2. If $n+1$ is not a prime number, then $n+1 = a \cdot b$ where a and b are positive integers, both different from $n+1$ and 1. Thus, $2 \leq a \leq n$ and $2 \leq b \leq n$. By the induction hypothesis, a and b can each be expressed as a product of prime numbers, say $a = p_1 p_2, \cdots p_r$ and $b = q_1 q_2 \cdots q_s$. Since $n+1 = a \cdot b = p_1 p_2, \cdots p_r q_1 q_2 \cdots q_s$, $n+1$ can also be expressed as a product of prime numbers, namely, the product of primes that multiply to give a times the product of primes that multiply to give b.

By the second principle of mathematical induction, every $n \geq 2$ can be expressed as a product of prime numbers. □

Discussion

In this example, the first principle of induction would be virtually impossible to apply, since the integer n is not a factor of $n+1$ when $n \geq 2$. That is, knowing the factors of n doesn't tell us anything about the factors of $n+1$.

3.7. Well-Ordered Sets.

DEFINITION 3.7.1. *A set S is* **well-ordered** *if every non-empty subset has a least element.*

Well-ordering Principle. The set $\mathbb{N}$ of natural numbers forms a well-ordered set.

Discussion

As we prove below, the principle of induction is equivalent to the *well-ordering principle*.

EXAMPLE 3.7.1. *The set S of integers greater than -5 is a well-ordered set.*

EXAMPLE 3.7.2. *The set P of rational numbers greater than or equal to zero is not a well-ordered set.*

EXAMPLE 3.7.3. $[0, 1]$ *is not well-ordered. The subset* $(0, 1]$ *does not have a least element in the set. (You may have to think about this for a moment.)*

EXAMPLE 3.7.4. *The set $\mathbb{Z}$ of integers is not well-ordered, since $\mathbb{Z}$, itself, does not have a least element.*

Study the proof of the following theorem carefully. Although it uses methods of proof discussed in *Module 3.2*, its level of abstraction may make it a bit difficult to absorb at first.

THEOREM 3.7.1. *The second principle of mathematical induction is equivalent to the well-ordering principle.*

PROOF. We must show that each principle implies the other.

1. Suppose $\mathbb{N}$ satisfies the principle of mathematical induction, and suppose that A is a nonempty subset of $\mathbb{N}$. We will give a proof by contradiction that A has a least element. Suppose A does not have a least element. Let $P(n)$ be the predicate $n \notin A$. Then
   (i) $0 \notin A$. Otherwise, 0 would be the least element of A. Thus $P(0)$.
   (ii) Let $n \in \mathbb{N}$. Suppose $P(k)$ for $0 \leq k \leq n$. Then $0, \ldots, n \notin A$. If $n + 1$ were in A, then $n + 1$ would be the least element of A. Thus, $n + 1 \notin A$, and so $P(n + 1)$. This proves that $P(0) \wedge \cdots \wedge P(n) \to P(n + 1)$.

   By the First Principle of Mathematical Induction, $\forall n P(n) = \forall n[n \notin A]$. But this means that A is empty, a contradiction. Thus $\mathbb{N}$ is well-ordered.
2. Suppose $\mathbb{N}$ is well-ordered, and suppose $P(n)$ is a predicate over $\mathbb{N}$ that satisfies the hypotheses of the First Principle of Mathematical Induction. That is,
   (i) $P(0)$, and

(ii) $P(0) \wedge \cdots \wedge P(n) \to P(n+1)$.

We will prove $\forall n P(n)$ by contradiction. Suppose $\neg \forall n P(n)$. Let A be the set of all $n \in \mathbb{N}$ such that $P(n)$ is false (i.e., $\neg P(n)$) Then A is nonempty, since $\neg \forall n P(n) \Leftrightarrow \exists n \neg P(n)$. Since $\mathbb{N}$ is well-ordered and A is a nonempty subset of $\mathbb{N}$, A has a least element k. In other words, if $P(n)$ fails to be true for all n, then there is a smallest natural number k for which $P(k)$ is false. By (i), $k \neq 0$, hence, $k > 0$, which implies $k-1$ is a natural number. Since $k-1 < k$, and k is the least element of A, $k-1 \notin A$, so that $P(k-1)$. But by (ii) $P(k-1)$ implies $P(k)$, or $k \notin A$, which contradicts $k \in A$. Therefore, $\forall n P(n)$, and so $\mathbb{N}$ satisfies the principle of mathematical induction.

$\square$